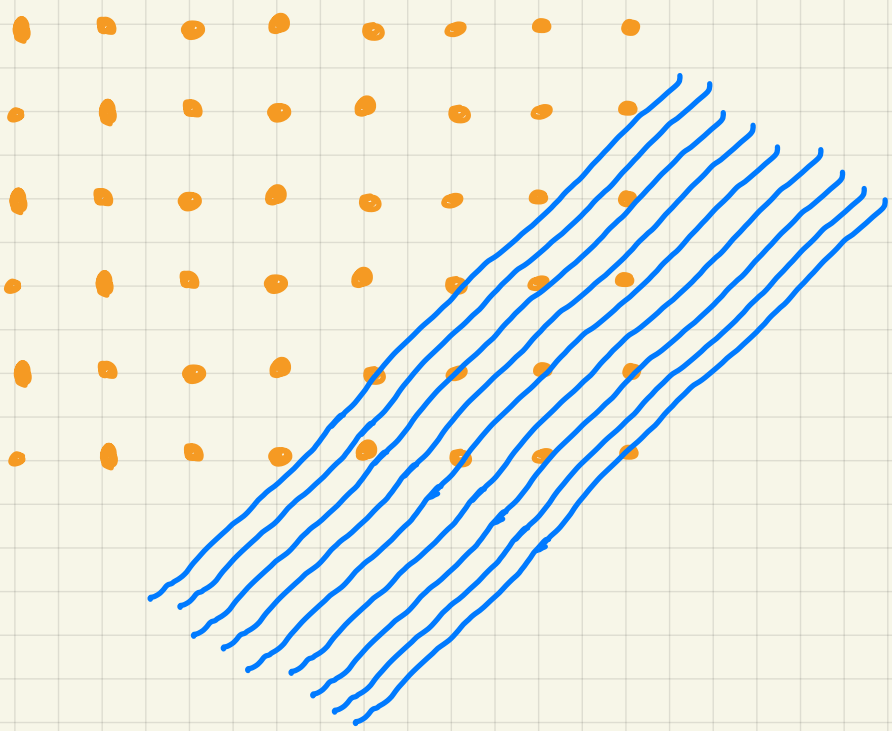
GDO-02 15.10.19

Für $a \in \mathbb{R}^n$, $\delta \in \mathbb{R}$: $H^{\leq/\geq/=}(a,\delta) := \{x \in \mathbb{R}^n : \langle a, x\rangle \leq/\geq/= \delta\}$

Beobachtung: Für $a \in \mathbb{Z}^n \setminus \{0\}$:

$$\mathbb{Z}^n = \bigcup_{\delta \in \mathbb{Z}} H^{=}(a,\delta) \cap \mathbb{Z}^n$$



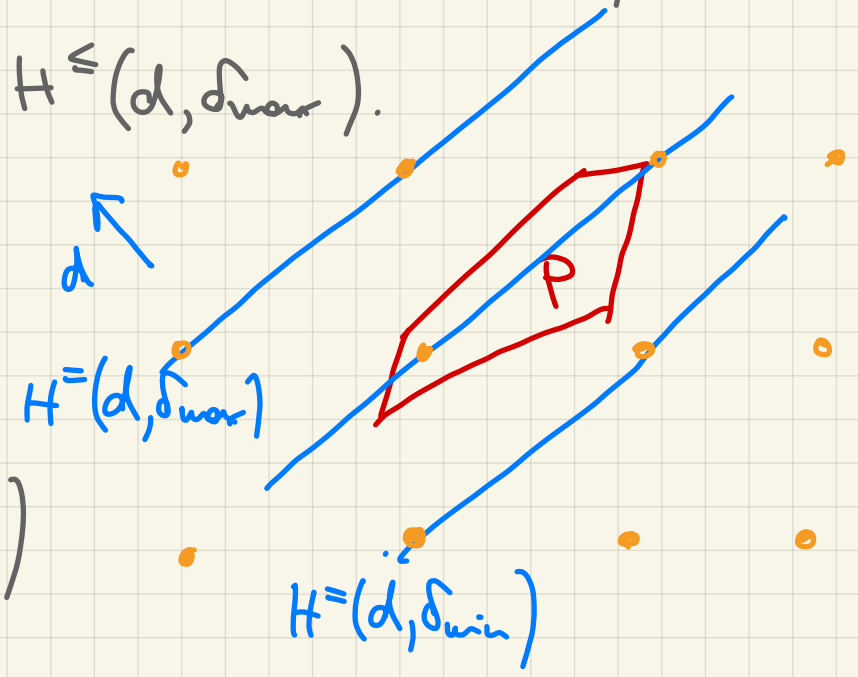
Lenstras Algorithmus (Grundidee) für IP-Zulässigkeit

⓪ Sorge dafür, dass $P^{\leq}(A,b)$ volldimensionales Polytop ist.

① Finde a) $x^* \in P^{\leq}(A,b) \cap \mathbb{Z}^n$ oder

b) $d \in \mathbb{Z}^n \setminus \{0\}$, $\delta_{min}, \delta_{max} \in \mathbb{Z}$ mit $\delta_{max} - \delta_{min} \leq k(n)$ und

$$P^{\leq}(A,b) \subseteq H^{\geq}(d,\delta_{min}) \cap H^{\leq}(d,\delta_{max}).$$



② Falls in ① a) nicht erreicht wurde:
Wende den Algorithmus rekursiv auf $\leq k(n)+1$ Instanzen

$$Ax \leq b, \quad \langle d, x \rangle = \delta_k \quad (k = 0, \dots, k(n))$$

der Dimension $n-1$ an.

Bemerkung: Gelingt es, Schritt ⓪ und ① für festes n in Polynomialzeit durchzuführen, so läuft der Algorithmus für festes n in Polynomialzeit (da für festes n auch $(k(n)+1)(k(n-1)+1)\cdots = \text{const}$ ist).

Polynomial in $\langle A, b\rangle$: Exponent des Polynoms darf von n abhängen

Hintergrund

Def.: Sei $K \subseteq \mathbb{R}^n$ konvex und kompakt.

(i) Für $d \in \mathbb{R}^n$: $w_d(K) := \max\{\langle d, x\rangle : x \in K\} - \min\{\langle d, x\rangle : x \in K\}$

(ii) $w(K) := \min\{w_d(K) : d \in \mathbb{Z}^n \setminus \{0\}\}$ ("Gitterweite" von K)

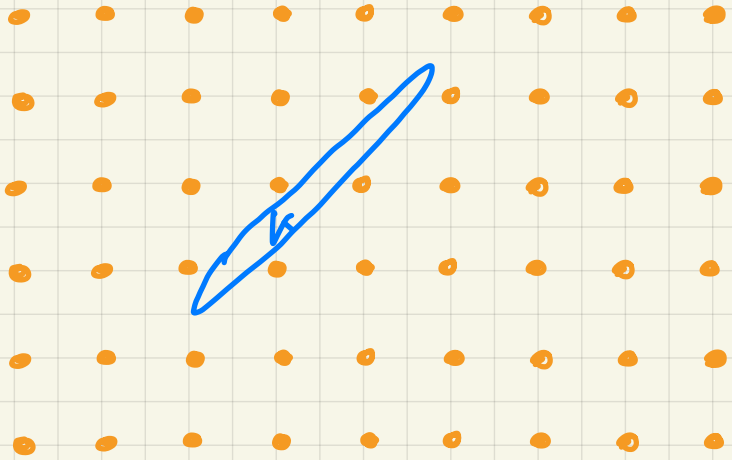
Khinchine's Flatness Theorem

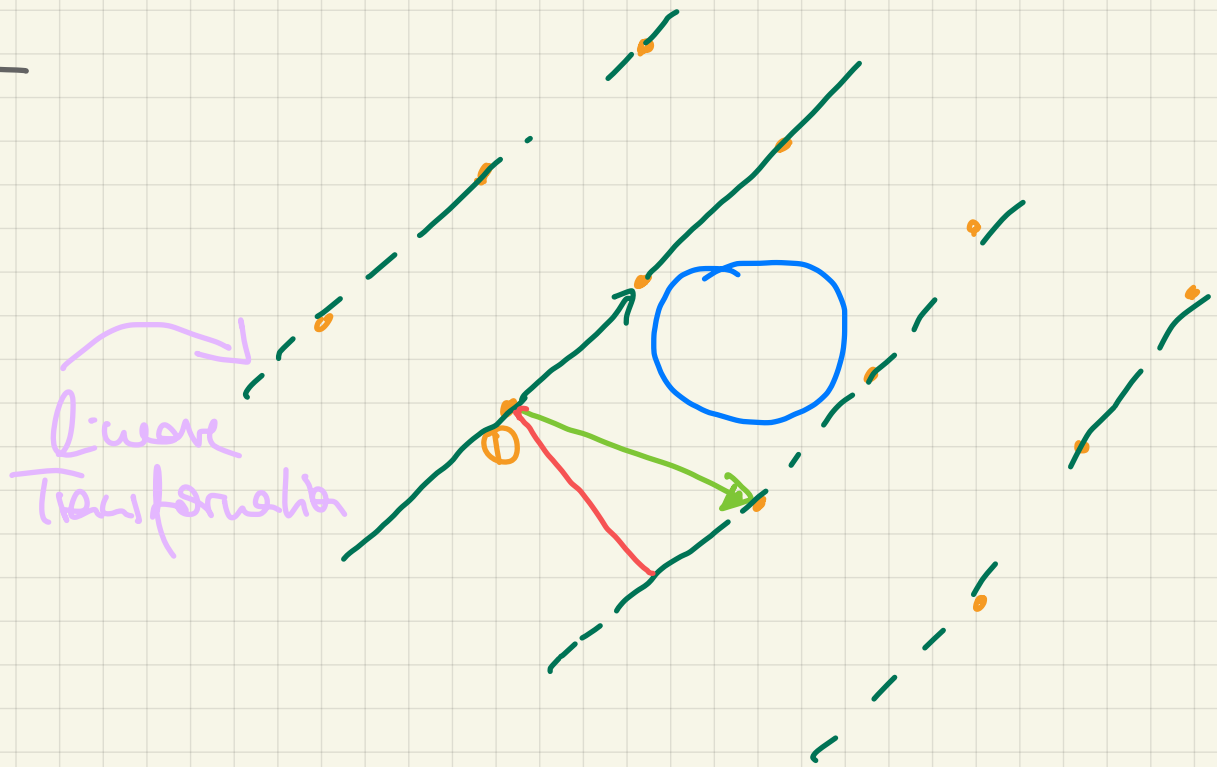
Es gibt $k : \mathbb{N} \to \mathbb{N}$, so dass für alle konvexen, kompakten Mengen $K \subseteq \mathbb{R}^n$ mit $K \cap \mathbb{Z}^n = \emptyset$

$$w(K) \leq k(n)$$

gilt.

Spezialfall: K = Ellipsoid



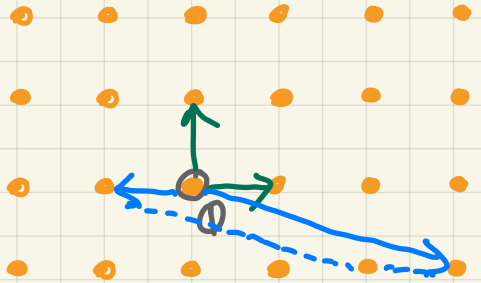


$\rightsquigarrow$ Finde den Gittertaus B des Gitters im rechten Bild mit einem ausgezeichneten Basisvektor $b^* \in B$, so dass die Höhe von b^* über $\lim(B \setminus \{b^*\})$ möglichst groß ist.

Def.: $\Lambda \subseteq \mathbb{R}^n$ ist ein n-dimensionales **Gitter**, wenn es eine reguläre Matrix $B \in \mathbb{R}^{n \times n}$ mit $\Lambda = B \cdot \mathbb{Z}^n =: \Lambda(B)$ gibt. Jede Basis B (bzw. die Menge der Spalten von B) heißt dann eine **Gitterbasis** von Λ.

Bem.:

- n linear unabhängige Vektoren im Gitter Λ bilden genau dann eine Gitterbasis von Λ, wenn die einzigen Λ-Punkte im aufgespannten Parallelepiped die Ecken sind.



- Für zwei reguläre Matrizen $B, B' \in \mathbb{R}^{n \times n}$ gilt genau dann $\Lambda(B) = \Lambda(B')$, wenn es eine unimodulare Matrix $U \in \mathbb{Z}^{n \times n}$ gibt mit $B' = BU$.